HARVARD LAW SCHOOL
NATIONAL SECURITY JOURNAL

Expanding Lawful Influence Operations

by Justin Malzac | Apr 12, 2022 | Online Edition

Justin Malzac[*]

[This essay is available in PDF at this link]

"It's always easier to stamp out a small ember than to put out a raging fire." [1]

— Lloyd Austin, Secretary of Defense

Introduction

Influence operations, including propaganda and psychological operations, have been a central aspect of international rivalry for over a century. Emphasis on this particular form of grey zone diplomacy and competition faded after the fall of the Soviet Union and the end of the Cold War, but we have witnessed a resurgence in recent years. The Center for American Progress notes that "[w]hile foreign influence operations are not new, the convergence of three larger global trends has made them a more important and acute challenge."[2] It attributes this increase in influence activity to the return of global great power competition, to the rise of nationalism and authoritarian governments seeking to exploit the openness of liberal democratic social systems, and to the digital revolution, which has exponentially increased the capability of actors to push information to wide audiences.

This new reality has manifested itself in a range of malign actions directed against the United States and its allies. For example, A recent assessment from the National Intelligence Council reported that Russia, Iran, Hezbollah, Cuba, and Venezuela all attempted, in some manner, to influence the 2020 presidential elections.[3] The report notes that "[a] key element of Moscow's strategy this election cycle was its use of people linked to Russian intelligence to launder influence narratives—including misleading or unsubstantiated allegations against President Biden—through U.S. media organizations, U.S. officials, and prominent U.S. individuals."[4] Russia has also been actively engaging in influence operations in Germany. As noted by The Center for Strategic and International Studies (CSIS), one of the more famous cases was a 2016 disinformation campaign centered on "a fabricated story about a Russian-German girl named Lisa who was supposedly raped by migrants. The 'Lisa case' sought to inflame xenophobia, galvanize the Russian-German community, and undermine support for [Chancellor] Merkel's immigration policy."[5] CSIS has also reported on

geopolitical influence efforts by China, most notably in Australia, that have become "a cautionary tale about the ways in which China seeks to covertly influence and interfere with the political process in advanced democracies."[6] Even North Korea is actively engaged in global influence operations. As reported in The Diplomat, "North Korea had about 7,000 agents engaged in this propaganda work as of the end of 2017, and it is adding more."[7] Much of this effort targets South Korea, a critical U.S. ally.

If you've been playing National Defense Strategy (NDS) bingo here, you'll notice that all five of the key adversaries laid out in the 2018 NDS are represented above—China, Russia, Iran, North Korea, and violent extremist organizations (VEOs) such as Hezbollah. All of the United States' primary global rivals are actively engaged in influence campaigns against the United States or its allies. It comes as no surprise, then, that interim national security guidance from the Biden administration has reiterated "[a]nti-democratic forces use misinformation, disinformation, and weaponized corruption to exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance. Reversing these trends is essential to our national security."[8]

Expanding lawful influence operations abroad is key to fulfilling the goals of the NDS. Active influence operations—often executed by the Department of Defense—support key defense objectives in the NDS, to include "[e]nabling U.S. interagency counterparts to advance U.S. influence and interests."[9] The diplomatic efforts of the Department of State can be strengthened by DOD actions to counter the problematic messaging of competitor states. Information operations support irregular warfare, or IW, which is defined as "a struggle among state and non-state actors to influence populations and affect legitimacy. IW favors indirect and asymmetric approaches . . . in order to erode an adversary's power, influence, and will."[10] T supported by influence operations. [11] As noted by Lieutenant Colonel Norman Emery, "In irregular warfare, non-lethal capabilities have a more prominent and necessary role than in conventional warfare. Information operations directly influence the irregular warfare operational focus—the relevant populations."[12] In presenting the IW Annex, the Acting Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict, or ASD(SO/LIC), argued "[t]o compete in the information environment, the United States must accept that influence is an integral aspect of modern warfare, not just a niche capability."[13]

So far, responding to malicious influence campaigns solely in a reactive manner has been insufficient to stem the tide, suggesting that a more aggressive and proactive strategy is required. Justice Louis Brandeis argued in his concurring opinion to *Whitney v. California*—a significant First Amendment case—that "[i]f there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence."[14] This can be viewed as a reformulation of the old adage that *the best defense is a good offense*. All states, especially democratic states like the US, are severely handicapped when it comes to disrupting or preventing malign influence operations against its population and social systems, especially when those actions fall below the threshold for a use of force. Part of this is the inherently open nature of democratic societies, with protections for freedom of expression and human rights. Because of these rights, democratic societies cannot simply shut off the spigot of

misinformation. In other words, as technology continues to give the edge to the offense, a purely defensive strategy will fail. The DOD has already shifted to an offense-oriented strategy in cyberspace, known as "defend forward,"[16] so it is not unreasonable to argue for a similar strategy of "influence forward" to deal with a threat that is just as severe, if not worse.

It is important, however, that any offensive influence operations undertaken by the United States or its allies are compliant with international law, because legitimacy is a key component of such messaging. A copious amount of ink has been spilt on malign influence activities directed at the United States, with much of this scholarship attempting to discern whether specific actions by adversary states violated international law.[17] Absent from the debate, however, is any notion on how the United States might pursue its own influence efforts within the lawful operating space. The focus in academia is consistently on what should not be done, rather than what can be done. This is a significant oversight that is worth addressing.

As adversaries continue to increase malicious information operations against the West, it is time for the United States to push back with lawful influence operations of its own. Influence operations are essential to supporting the national defense strategy and policy, and as this paper will show, there is plenty of space to execute them lawfully**.**

I. A Brief History of American Influence

The United States, as with most global powers, has a long history of engaging in "influence operations." A 2009 RAND study provides a working definition for influence operations, suggesting that

Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further [state] interests and objectives.

This provides a comprehensive sense of the extent of the term, but it is rather unwieldy for the purposes here. Thankfully, Duncan Hollis has provided a more expedient definition, suggesting that an influence operation is "a deployment of resources for cognitive ends that foster or change a targeted audience's behavior."[19] Influence operations specifically target the human mind and seek to promote changes in the target audience's behavior to support political goals. As such, they can be distinguished from intrusive cyber operations that manifest effects on networks and systems, or even cause physical damage. Rather, influence operations target the "social " of a select target audience, with the intent to change deeply held thoughts and beliefs, rather than the structure of data.[20]

As early as 1947, congressional representatives were lamenting the state of the United States' reputation abroad, which was being undermined by the influence operation efforts of the Soviet Union.[21] This led to legislation putting the State Department in control of a peacetime media program abroad, and established U.S. state media as "a pillar of U.S. foreign policy."[22] What followed was the creation, in the decades to come, of broadcasters such as Voice of America (VOA)

and Radio Free Europe (RFE). Contrary to Soviet propaganda campaigns, which were often blatantly false, U.S. state media entities "strived to produce trustworthy media content based on facts."[24] In the 1990s, U.S. state media broadcasting expanded to new crisis areas in the Middle East and Central Asia, and the entities "began to devote additional resources to more modern forms of communication" such as the internet.[25]

Tim Weiner's comprehensive history of the Central Intelligence Agency includes a quote from former U.S. Secretary of Defense Robert Gates who argued that "became the first president since Truman to challenge directly the legitimacy of the Soviet government in the eyes of its own people." This was accomplished by, among other things, publishing magazines, distributing dissident writings, and handing out cassette tapes to "free minded people behind the iron curtain."[27] Indeed, it was the subtlety of these actions—as compared to the prior flagrant covert actions that violated international law and sovereignty—that increased their effectiveness. As Weiner argues, Carter's "modest mobilization of the CIA to probe that weak chink in the armor of the iron curtain was a cautious challenge to the Kremlin. Nevertheless, he hastened the beginning of the end of the Soviet Union."[28]

U.S. influence operations have never been restricted solely to efforts by the State Department and the CIA, however. Since the Korean War, the Department of Defense has actively engaged in influence operations in the form of leaflet drops, radio broadcasts, social media engagements, and more, because "technological advances continue to provide innovative media and delivery methods to convey messages to" target audiences. Indeed, propaganda and influence operations have a long and enduring history within the military. During the first 125 days of the Korean War, more than 100 million propaganda leaflets were disseminated; within days of the outbreak of war, 19 radio transmitters in Japan were broadcasting onto the Korean peninsula.[30] In more recent times, influence operations and psychological operations have been employed substantially in the War on Terror. [31] One RAND study suggested that, though regular Afghans were against the idea of terrorist training camps in their country, "until U.S. forces arrived and proclaimed it, there was little belief among the main Pashtun target audience that Afghanistan had become a safe haven for international terrorists."[32]

The problems of malign influence during the Cold War, to which influence operations were sometimes deftly applied, have returned to the modern world of global power competition. "[33] above, expanding lawful U.S. influence operations is in line with current national security policy, and there is a significant role for the DOD to play in this effort. In the Fiscal Year 2020 National Defense Authorization Act (NDAA), Congress clarified DOD's authority to conduct information operations "to defend the United States, allies of the United States, and interests of the United States, including in response to malicious influence activities carried out against the United States or a United States person by a foreign power."[34] However Major Coombs warns that the influence component within special operations is undermanned and deemphasized, losing out to counterterrorism priorities such as hostage rescue and direct action. Considering the onslaught of malign influence the nation currently faces, this trend of ignoring influence capabilities in the military must be reversed.

Along with a renewed emphasis on offensive information operations, it is critical to understand the landscape of international law relevant to such activities, to ensure they are conducted in lawful manner. As noted previously, this is critical for safeguarding the legitimacy and trust of the United States, factors that will directly affect how a target audience receives any potential messaging. The rest of this article examines the application of international law to influence operations and applies that assessment to a case study.

II. International Law Relevant to Influence Operations

On October 7, 2020, the Department of Justice announced the seizure of 92 domain names that were being used by Iranian agents to spread disinformation and propaganda.[36] Some of these sites were disguised as legitimate news platforms, despite being controlled by the government of Iran for the sake of disseminating propaganda. [37] The enforcement action was taken under domestic authorities, such as the *International Emergency Economic Powers Act*, ,[38] .[39] Interestingly, no claim was made that the Iranian actions were violations of international law. The United States reacted more severely to Russian election interference and hacking in 2016, with the expulsion of 35 diplomats and other sanctions enacted by the Obama administration against Russia. [40] Imposing sanctions, expelling diplomats, and other such actions are classic retorsions used by states to respond to perceived violations of international law. Though the Obama Administration did not explicitly state that these actions were a response to a violation of international law, the use of these retorsions instead of traditional domestic law enforcement may indicate that the Administration viewed Russian actions as contrary to international law.

The customary law and treaty law which may be applicable to a particular influence operation are largely dependent on the dissemination method employed for such an operation. On one end of the spectrum, international regulation of radio transmission tends to reflect a generally-recognized right of free information by preventing interference by states instead of restricting states' ability to broadcast. Resolution 424 of the fifth UN General Assembly is perhaps one of the most specific measures related to state radio broadcasts. The resolution affirms "the right of all persons to be fully informed concerning news, opinions and ideas regardless of frontiers" and "[i]nvites the governments of all Member States to refrain from such interference with the right of their peoples to freedom of information," with the caveat that states should "refrain from radio broadcasts that would mean unfair attacks or slanders against other peoples anywhere." A very different influence operation on the other end of the spectrum would be leaflet drops by aircraft crossing into a rival state's territorial airspace, which would violate numerous aspects of sovereignty, and could even be perceived as a use of force. Cyber operations, including the use of social media, fall somewhere between these two extremes, though the exact application of sovereignty rules on cyber operations is still debated. Regardless of the method, however, any messaging directed at a population must be assessed through the lens of state sovereignty and, more importantly, the principle of non-intervention.

III. The Principle of State Sovereignty

State sovereignty in its modern form flows from the idea that the state has exclusive control over its territory and inherent functions. The long-established Lotus Principle provides that internal sovereignty of states is only constrained by those rules which states adopt freely, such as treaties. [43] More and more, modern states are ceding their sovereign powers for the sake of global security through treaties like the *U.N. Charter*, in which Article 2(4) requires "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[44]

The Charter is the cornerstone of the modern *jus ad bellum* construct. It is well-established that absent self-defense justifications, actions constituting hostile uses of force in any form, whether they be kinetic strikes or cyber operations, violate the Charter and international law. What is less clear, and has been argued ad nauseum in recent years, is how sovereignty applies to actions which are not uses of force, such as non-destructive cyber or influence operations. As noted by Christopher Stein, an Air Force and Space Force judge advocate,

The *jus ad bellum* is primarily concerned with bringing the level of interstate violence to zero. It is much less concerned with those activities that fall below the threat or use of force . . . it certainly does not purport to eliminate all forms of coercion between states. In fact, one might hypothesize that because interstate competition is inevitable, banning force is likely to increase other forms of conflict as the competition is channeled to nonviolent forums.[45]

Indeed, the Charter itself is not particularly helpful in addressing the lawfulness of operations below the threshold for use of force. Instead, customary international law (CIL) is relied upon. The existence of is proven by "evidence of general practice, and evidence of a belief the practice is required by international law (the *opinion juris* element)."[46] The aspects of CIL applicable to influence operations are those of territorial sovereignty and non-intervention.

With computers or any telecommunications, there are systems and nodes that are physically located in one state or another. Does an operation routing through one of those nodes then always implicate the principle of sovereignty? State *opinio juris* is split on the issue. The French government has argued that "any unauthorized penetration" of systems in a state's territory "via a digital vector *may* constitute, at the least, a breach of sovereignty."[47] The position of the United States, however, is less strict. U.S. officials have consistently argued that there is no strict rule of sovereignty in international law, particularly in relation to networks, and therefore not all intrusions are violations of sovereignty.[48] For example, a 2017 memo from then-DOD General Counsel Jennifer O'Connor argued that territorial sovereignty, at least in relation to information operations, is "an organizing principle of international law, foundational, yet lacking independent or substantive legal effect."[49] Rather, the U.S. perspective, and that of many other countries, is to apply an effects-based approach to analyzing whether information operations violate international law or norms.[51]

When there is a physical intrusion into the territory of another state, the principle of sovereignty is more clearly implicated.[52] For example, if state agents launch leaflet-carrying balloons across the border (as the North Korean military often does) the sovereignty of the victim state may be violated. [53] Moreover, in such a case, treaty law may be implicated, such as the *Chicago Aviation*

Convention[54] or the *Korean Armistice Agreement*.[55] Things are not so simple, however, when assessing actions in the information space, where there may be no physical intrusion at all. In the case of non-intrusive influence operations—whether via radio, social media, or other methods—the principle of sovereignty tends to lack utility or clarity in application. Therefore, an effects-based analysis, and an effects-oriented rule, is required to assess the legality of such operations. This brings us to non-intervention.

A. The Principle of Non-Intervention

Non-intervention as a principle of international law has a much shorter history than that of the principle of sovereignty. Stephen Townley provides a concise history of the development of the principle, noting that the United States first accepted the doctrine with the *Montevideo Convention* in 1933.[56] The concept was then adopted in the 1948 *Charter of the Organization of American States*. The *U.N. Charter* did not include non-intervention provisions[57], and this gap wasn't addressed until 1970, with the *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States Declaration*").[58]

Non-intervention as a fundamental principle of international law was most clearly elucidated in the decision of the International Court of Justice (ICJ) in the now infamous *Nicaragua Case*. In this landmark case, the ICJ explained

[T]he principle forbids all states or groups of states to intervene directly or indirectly in internal or external affairs of other states. A prohibited intervention must accordingly be one bearing on matters in which each state is permitted, by the principle of state sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[60]

It has since been generally agreed that non-intervention hinges on two factors: 1) the interference is related to those matters which are exclusively under the domestic control of the victim state, and 2) the influence is coercive in nature. Those matters to which each state is permitted to decide freely are the "*domaine réservé*" of the state.

B. Domaine Réservé

"[M]atters on which international law does not speak or that international law leaves to the prerogative of states are considered *domaine réservé* and therefore protected from intervention by other states." The principle of non-intervention applies to, among other things, a state's "political, economic, and social system[s]."[62] This has been interpreted to include any aspect of elections or politics in an individual state's *domaine réservé*.[63]

Interventions in domestic elections must target or affect the electoral process, such as by tampering with voting machines or attacking candidates through hacking or blackmail. Managing electoral processes is the exclusive domestic right of the state.[64] Recently, a group of international law experts published a statement on electoral interference. In this statement, the authors and other signatories assert that "international law applies to cyber operations by states, including those that

have adverse consequences for the electoral processes of other states." The authors defined "adverse consequences" in the electoral context as "actions, processes or events that intervene in the conduct of an electoral process or undermine public confidence in the official results or the process itself."[66] They also argue that states have a duty to refrain from actions which have adverse consequences, including "conducting operations that violate the right to privacy, freedom of expression, thought, association, and participation in electoral processes."[67]

However, there is a strong difference between actions that disrupt state processes (e.g., hacking of election machines) or violate privacy rights (e.g., personal email leaks), and those that only seek to influence public opinion. The minds of the people and public opinion (or the social imaginary) are not the property of the state, nor a function of the state. Rodriguez argues, citing the *Tallinn Manual*, that coercive intervention "must be distinguished from persuasion or propaganda. These activities merely involve influencing."[68] This seems to be why the Russian hacking of candidates and disruption of electoral processes in 2016 were treated as breaches of international law, whereas Iranian passive messaging through pseudo-news websites in 2020 were not (though still violations of domestic law).

The restriction against interfering in the elections and political processes of a state also inherently prohibits acts which fundamentally change those processes (i.e., regime change). In *Nicaragua*, the ICJ "if one state, with a view to the coercion of another state, supports and assists armed bands in that state whose purpose is to overthrow the government of that state, that amounts to an intervention by the one state in the internal affairs of the other."[69] Such prohibited support may include "financial support, training, supply of weapons, intelligence and logistic support."[70] The *Friendly Relations Declaration* and other international agreements establish an affirmative duty for states to refrain from instigating civil unrest or uprisings in other states. Among other things, the declaration establishes, *inter alia*, that "states have the duty to refrain from propaganda for wars of aggression," that "every state has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another state," and that "every state has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another state."[71] Although not a treaty in and of itself, the ICJ in *Nicaragua* argued that the declaration was representative of customary international law due to the fact that U.N. member states publicly consented to the language therein.[72]

That's not to say that what falls into the category of *domaine réservé* is strictly clear. Townley notes that "it has been accepted since the Permanent Court of Justice's decision in the *Nationality Cases* that the *domaine réservé* is variable based on a state's international obligations, which necessarily means that its boundaries may differ as between states and may change over time."[73] For example, intervention to pressure a state to conform to an international norm, a treaty obligation, or to enforce a UN Security Council resolution, would fall outside the *domaine réservé* and would not violate the principle of non-intervention.

C. Coercion

In order to violate the principle of non-intervention, influencing must not only touch on matters in the *domaine réservé* but must also be coercive in nature. As noted by the ICJ in *Nicaragua*, "intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[74] Unfortunately, the ICJ did not provide a clear definition of coercion short of noting that "the element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force."[75] Influence operations typically fall below the threshold for use of force, so this caveat is not useful in evaluating the present issue. Indeed, defining coercion is perhaps even a more ambiguous and contentious issue than that of *domaine réservé*.

Much of the debate in the 1980s, before and after *Nicaragua*, fixated on economic coercion and leaned on state intent being a primary factor—when the intent of an economic embargo was to generate political effects, rather than simply dealing with specific trade issues, the action might constitute unlawful intervention.[76] However, more recent scholarship has viewed coercion through an effects-based assessment. Manuel Rodriguez has argued that "coercion must have the potential to compel the target state to engage in an action that it would otherwise not take, or to refrain from taking an action that it would otherwise take."[77] Referencing the *Tallinn Manual*, Rodriguez suggests "disabling election machinery by a cyber [or] information operation would result in the manipulation of the election and give rise to coercion."[78] Therefore, coercion applies to actions by one state that undermine the free will of the victim state to control state functions.

Regarding influence operations, Hollis suggests "the very nature of [influence operations]—the goal of having a target adopt or change certain behaviors willingly—implies an absence of coercion."[79] The authors of the *Tallinn Manual* also warned that coercion, and therefore intervention, must be separated from mere propaganda or influencing.[80] Hollis offers a few examples of when information operations might cross the threshold into coercion. These include "the 2015 BlackEnergy Operation that took down parts of the Ukrainian power grid" or a hypothetical "distributed denial of service attack targeting a state's banks"—which, far from being merely rhetorical, was exactly what happened in Tallinn, Estonia, in 2007.[81] But, Hollis notes, typical influence operations "are not about coercing targets into capitulation or wearing them down, but rather convincing them to adopt—seemingly on their own—some attitude, view, or behavior that the [influence operations'] authors favor."[82] Thus, the assessment of coercion hinges on issues beyond a mere attempt at influence, to the techniques and effects involved. Again, we can see why the Russian efforts in 2016—which included hacking, network disruptions, and timed leaks of personal correspondence with an aim to disrupt electoral processes—was an affront to international norms, whereas passive Iranian websites were . Influence operations that coercively affect the free will of states to perform their government functions, such as elections, will run afoul of international legal norms. But even within these limitations, a wide maneuver space for lawful influence operations remains.

III. Case Study: North Korea

The glimmer of hope for improved relations between the United States and North Korea, and for reduced tensions on the Korean Peninsula, peaked with the Hanoi Summit in February of 2019.

Recently, the situation has all but returned to the status quo prior to the brief *détente*. Worse, many have argued that the U.S. pressure campaign and associated sanctions—intended to push the North Korean leadership away from nuclear weapons and ballistic missiles, and back to the negotiating table—have been ineffective.[83] This has led pundits and national security analysts to offer a myriad of new proposals for tackling this enduring issue.

One such idea was promoted by a well-known military scholar. A colonel in the United States Army, Shawn Creamer served for many years in South Korea as a mid-level commander and a senior staff planner. He is recognized by many as the preeminent expert on the complex U.S. military command and control structures in the theater, having produced several academic works on the topic.[84] In 2020, as North Korean leader Kim Jong-un rejected calls for further meetings with U.S. leaders, and returned to past aggressive behavior and rhetoric, Creamer penned an unofficial article urging a more aggressive policy towards the north. He suggested:

One such higher-risk, alternative option worthy of further study is to aggressively use American overt and covert elements of national power to purposefully facilitate a change in North Korean leadership. Facilitating a "transformed regime" is not regime change emanating from an external decapitation strike or the forcible removal of the Kim family regime by outside powers, and all the associated baggage that comes with a military campaign, occupation and nation-building. Rather, this alternative approach is pursuit of a deliberate policy to foment instability within the regime, and encouraging regime elites to change their leadership.[85]

Ultimately, what he is arguing for here is an influence campaign, rather than a kinetic "decapitation strike" or forceful "military campaign."[86] Indeed, what he proposes seems to fall neatly into the RAND definition of influence operations. The above perspective may come through the eyes of a former commander and a senior military planner with a desire to "lean forward" operationally,[87] and such officers should not be discouraged from thinking aggressively and proactively. In the end however, assessing the legality of such plans "falls to judge advocates and civilian attorneys at the tactical and operational levels."[88]

Unfortunately, the above proposal as written is largely unsupportable. At its core, Colonel Creamer's proposal is to employ elements of U.S. national power short of armed force (i.e., influence operations) to change the North Korea's national leadership (i.e., regime change). As the international law analysis above has shown, the choice of national leadership falls within the *domaine réservé*, and efforts to affect this choice would constitute prohibited intervention. Moreover, "a deliberate policy to foment instability within the regime"[90] would likely violate one of the tenets of the *Friendly Relations Declaration*, namely that "every state has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife."[91] It would also be coercive, in that the United States would be subjugating the will of the North Korea to freely choose its political systems by forcing a shift in leadership away from the Kim family. This means that the general scheme presented by Colonel Creamer is unviable from a legal standpoint.

On the other hand, if the change urged by U.S. messaging focuses on compliance with international law, the principle of non-intervention would not be violated, as matters to which international law

speaks and imposes obligations on the state are not *domaine reserve*. The idea of "stimulating internal forces to alter the direction North Korea is moving" does not have to be bound, hand and foot, to a policy of regime change. The launch of ballistic missiles by the North violates standing U.N. Security Council resolutions, as do nuclear weapons testing, exports of coal, and numerous other behaviors. The Institute for Science and International Security "identified over 250 alleged violations" of UNSC sanctions by North Korea in a single year.[92] North Korean armed attacks on the South violate international obligations and duties with respect to the *U.N. Charter* and the *Korean Armistice Agreement*. Influence with the intent to convince North Korean leaders to comply with these international rules would not constitute intervention. There is, therefore, certainly room for overt and covert influencing in the United States' approach to North Korea.

Such influence operations would clearly be in line with the national security policy of the United States. The Interim National Security Strategic Guidance specifically calls for activities which "empower our diplomats to work to reduce the threat posed by North Korea's growing nuclear and missile programs."[93] The DOD could be employed—in coordination with the Department of State and supporting the NDS—to craft messages and products targeting decision makers in North Korea who can influence the cycle of military escalation by the North. These messages could be disseminated by non-intrusive means, such as radio or cyber, rather than physical means like balloon leaflet launches, which would likely violate the armistice and North Korea's sovereignty. This effort could also be reinforced by diplomatic outreach. Moreover, these effects might also be lawfully applied to China, a state that continues to violate international law by helping North Korea avoid sanctions and even "helping North Korea launder money from cyber thefts carried out to raise funds for its weapons programs."[94]

Clearly lawful influence operations such as those described above would help the United States regain some of the information space which has been lost to global competitors in recent years. The above example would only be a drop in the whole-of-government bucket needed to douse the flaring ember of misinformation, disinformation, and influence efforts of global competitors. But by starting with a single focused issue, such as the one described above, operators can begin to develop templates to apply to other areas, including Iranian proxy wars, Where strategic competitors act in violation of international norms, the United States can lawfully apply its information capabilities to influence a return to compliance. The DOD needs to start seriously thinking about how to employ influence as a strategic weapon, alongside new "laser weapons, high-powered microwave weapons and hypersonic weapons".[98]

Conclusion

The above case study is only one small example in an ocean of possibilities. Similar operations could be developed in reference to China, Russia, Iran, or VEOs. As long as these global competitors engage in behavior that violates international law and norms, the United States will be justified in employing influence operations against such behavior. The nation only requires the courage and capability to do so. This shift in strategic thinking needs to happen soon.

As noted in the National Defense Strategy, "For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested."[99] This includes the information domain. The United States is struggling to regain the dominance it once had in the influence space.[100] There is clearly room in strategic operations for lawful influencing, particularly when the messaging serves the purpose to encourage compliance with international law and norms.

The Department of Defense is currently engaged in a variety of messaging efforts across the globe. For example, USSOCOM recently established the Joint MISO WebOps Center, which "supports the combatant commands with improved messaging and assessment capabilities, shared situational awareness of adversary influence activities, and coordinated internet-based MISO globally." Some have argued, however, that current efforts are not enough, or even that the DOD views information operations as a mere "afterthought."[102]

Some of that aversion might reflect considerations of the risk that the United States might be viewed as violating international law by pushing propaganda. The term "propaganda" has taken on a pejorative tone for many, despite the clear ambiguities of the term. It would be prudent and helpful, therefore, to thoroughly assess the legal limits of such efforts, so that judge advocates and commanders can be certain they are operating lawfully. To adapt the words of former Secretary of Defense James Mattis,[104] clarity is needed to ensure we operate in the legal mid-field of international norms, rather than by skirting the sidelines. By establishing why such operations are lawful and justified, a critical pillar of national security policy—counter malign influence—can be reinforced.

---

[*] Justin Malzac is the Senior Paralegal at a DOD joint command and has been working in the national security law field for almost ten years. He has an M.A. in History from Pittsburg State University, a B.A. in English from the University of Minnesota, and was previously published in the *National Security Law Brief* and the *International Journal of Korean Studies.* The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the United States Army, the Department of Defense, or the United States Government. The author would like to graciously thank Majors Katherine Spencer and Leslie Schmidt, both judge advocates, for their inputs on this paper. This work would not have been possible without their mentorship.

[1] Lloyd Austin, Sec'y of Def., Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command (Apr. 30, 2021), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/ [https://perma.cc/554V-PUDG].

[2] Carolyn Kenney, Max Bergmann & James Lamond, *Understanding and Combating Russian and Chinese Influence Operations*, Ctr. for Am. Progress (Feb. 28, 2019), https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/ [https://perma.cc/XH2U-FJKV].

[3] *See* Nat'l Intel. Council, Foreign Threats to the 2020 U.S. Fed. Elections 1 (Mar. 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf [https://perma.cc/65DK-G5EP].

[4] *Id.* at 2.

[5] Jeffrey Mankoff, *Russian Influence Operations in Germany and Their Effect,* Ctr. for Strategic & Int'l Stud. (Feb. 3, 2020), https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect [https://perma.cc/N3ER-F4HP].

[6] Amy Searight, *Countering China's Influence Operations: Lessons from Australia*, Ctr. for Strategic & Int'l Stud. (May 8, 2020), https://www.csis.org/analysis/countering-chinas-influence-operations-lessons-australia [https://perma.cc/F6U6-BJUX]

[7] Tae-jun Kang, *North Korea's Influence Operations, Revealed,* Diplomat (Jul. 25, 2018), https://thediplomat.com/2018/07/north-koreas-influence-operations-revealed/ [https://perma.cc/TFV6-R7P3].

[8] The White House, Interim Nat. Sec. Strategic Guidance 7 (Mar. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf [https://perma.cc/85LU-84EN].

[9] Dep't of Def., Summary of the 2018 National Defense Strategy of the United States of America 4 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/2CWY-93R3].

[10] Dep't of Def., Summary Of The Irregular Warfare Annex To The National Defense Strategy 2 (2020), https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF [https://perma.cc/L63N-JT4T].

[11] *See id.* The IW Annex notes that IW-supporting "activities such as military information support operations [modern jargon for military influence operations] . . . also shape the information environment and other population-focused arenas of competition and conflict." *Id.*

[12] Norman E. Emery, *Irregular Warfare Information Operations: Understanding the Role of*

People, Capabilities, and Effects, Mil. Rev. 27 (Nov–Dec 2008), https://apps.dtic.mil/sti/pdfs/ADA547305.pdf [https://perma.cc/DV83-YBXF].

[13] David Vergun, *Great Power Competition Can Involve Conflict Below Threshold of War*, DOD News (Oct. 2, 2020), https://www.defense.gov/Explore/News/Article/Article/2364137/great-power-competition-can-involve-conflict-below-threshold-of-war/ [https://perma.cc/LU3U-MLHY].

[14] Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring). *See also* Herbert Lin, *On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations*, 15 I/S: J. L. & Pol'y for Info. Soc'y 1, 39 (2019).

[15] Bruce Schneier, *8 Ways to Stay Ahead of Influence Operations*, Foreign Pol'y (Aug. 12, 2019), https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/ [https://perma.cc/NM97-64BC].

[16] *See generally* Nina Kollars & Jacquelyn Schneider, *Defending Forward: The 2018 Cyber Strategy Is Here*, War on the Rocks (Sept. 20, 2018), https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.

[17] *See, e.g.*, Michael Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, Just Sec. (Dec. 21, 2020), https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [https://perma.cc/DK6L-DE4E] (Providing a convincing argument that the recent digital supply chain hacks by Russian agents were not violations of international law). These acts were analogous to traditional espionage which did not result in a use of force, nor coercive intervention, and thus do not allow severe international responses such as countermeasures. They were, however, certainly violations of U.S. domestic law, such as 18 U.S. Code § 1030.

[18] Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities,* Rand Corp. 2 (2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf [https://perma.cc/5ZX2-5HYF].

[19] Duncan Hollis, *The Influence of War; The War for Influence*, 32 Temple Int'l & Comp. L.J. 31, 36 (2018).

[20] "The Imaginary" is a term in sociology referring to "the set of values, institutions, laws, and symbols common to a particular social group and the corresponding society through which people imagine their social whole." *See* Brigitte Nerlich, *Imagining Imaginaries*, Univ. Nottingham Blogs (Apr. 23, 2015), https://blogs.nottingham.ac.uk/makingsciencepublic/2015/04/23/imagining-imaginaries/[https://perma.cc/9KMR-UUQD].

[21] Jennifer M. Grygiel & Weston R. Sager, *Unmasking Uncle Sam: A Legal Test for Defining and Identifying State Media,* 11 U.C. Irvine L. Rev. 383, 391 (2020).

[22] *Id.* at 392.

[23] *Id.* at 402.

[24] *Id.*

[25] *Id.* at 395.

[26] Tim Weiner, Legacy of Ashes: The History of the Central Intelligence Agency 416 (2007).

[27] *Id.*

[28] *Id.* at 418.

[29] Joint Chiefs of Staff, JP 3-13.2: Mil. Info. Support Operations, at I-6 (Nov. 21, 2014).

[30] Psychological Warfare in Korea: An Interim Report, 15 Pub. Op. Q. 65, 68, 73 (Spring 1951).

[31] Arturo Munoz, RAND Nat'l Def. Rsch. Inst., U.S. Mil. Info. Operations in Afghanistan: Effectiveness of Psych. Operations 2001-2010 38 (2012).

[32] *Id.* at 39.

[33] Robert Coombs, *Psychological Warfare: Principles for Global Competition*, Small Wars J. (Apr. 21, 2021, 12:15 PM), https://smallwarsjournal.com/jrnl/art/psychological-warfare-principles-global-competition [https://perma.cc/6ASJ-96ED].

[34] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1631, 133 Stat. 1742 (2019), codified at 10 U.S.C. § 397 note (b)(1) (2020).

[35] Coombs, *supra* note 33.

[36] Press Release, U.S. Dep't of Just. Off. of Pub. Aff., United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps (Oct. 7, 2020), https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps [https://perma.cc/AX9X-N2RG].

[37] *Id*.

[38] Exec. Order No. 13,876, 84 Fed. Reg. 30,573 (Jun. 24, 2019) (citing the International Emergency Economic Powers Act (50 U.S.C. § 1701 *et seq.*), the National Emergencies Act (50 U.S.C. § 1601 *et seq.*), the Immigration and Nationality Act of 1952 (8 U.S.C. §1182(f)), and 3 U.S.C. § 301).

[39] 22 U.S.C. § 611.

[40] Lauren Gambino et al., *Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking*, Guardian (Dec. 30, 2016), https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack [https://perma.cc/7H4F-ZW6L].

[41] *See, e.g.,* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 Cornell L. Rev. 565, 642 (2016). In defining the elements of customary international law and lawful responses to violations, Crootof notes "retorsions are politically unfriendly but always lawful self-help measures like discontinuing development aid, declaring a diplomat persona non grata, or imposing unilateral sanctions." *Id.* at 580 (emphasis removed). For another argument in favor of classifying Russia's actions as violative of international law, see Steven J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, Just Sec. (March 29, 2018), https://www.justsecurity.org/54340/shades-grey-russian-ops-violate-international-law.

[42] U.N. GAOR, 5th sess., suppl. no. 20, U.N. Doc. A/RES/424(V) (Dec. 14, 1950).

[43] S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) ("International law governs relations between independent States. The rules of law binding upon States therefore emanate

from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.")

[44] U.N. Charter art. 2(4). Article 2(7) of the Charter does not, as some argue, expressly prohibit inter-state intervention. *See infra* note 57.

[45] Christopher Stein, Hacking The Electorate: A Non-Intervention Violation Maybe, But Not an "Act Of War", 37 Ariz. J. Int'l & Comp. Law 29, 39 (2020).

[46] Steven Wheatley, Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About "Coercion", 31 Duke J. Comp. & Int'l L. 161, 172 n. 67 (2020).

[47] Ministere des Armees, International Law Applied to Operations in Cyberspace 6 (2019) (emphasis added).

[48] Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, U.S. Dep't of State (Nov. 10, 2016), https://2009-2017.state.gov/s/l/releases/remarks/264303.htm [https://perma.cc/L8NX-3TTD] (stating "remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations," especially when they have *de minimis* effects.).

[49] The DOD GC memo has since been pulled from public access, necessitating secondary citation. Sean Watts and Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 Lewis & Clark L. Rev. 771, 827 (2018).

[50] The U.K. shares this view. *See* Jeremy Wright, *Cyber and International Law in the 21st Century*, Gov.UK (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [https://perma.cc/WUZ5-MFKL].

[51] See also, Paul Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,* U.S. Dep't of Def. (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ [https://perma.cc/6W32-YP8Q]. Ney provides a detailed framework for the legal analysis, asking, "What is the military objective we seek to achieve? What is the operational scheme of maneuver and how does it contribute to achieving that objective? Where is the target located? Does the operation involve multiple geographic locations? What is the target system used for? How will we access it? What effects—such as loss of access to data—will we generate within that system? How will those effects impact the system's functioning? Which people or processes will be affected by anticipated changes to the system's functioning? Are any of those likely to be impacted civilians or public services?"

[52] Some have argued that "a state with an agent physically present in another state's territory who is exercising state powers within the territory of that other state without consent *may* be committing a violation of the latter state's sovereignty." Harriet Moynihan, The Application of International Law

to State Cyberattacks: Sovereignty and Non-Intervention 56 (2019) (emphasis added). *But see* Ney, *supra* note 51 (referring to the seemingly conflicting accepted state practice of espionage via agents in foreign territory).

[53] The actual altitude for which a state can claim territorial sovereignty is still debated. *See, e.g.*, Dean N. Reinhardt, *The Vertical Limit of State Sovereignty*, 72 J. Air L. & Com. 65 (2007).

[54] *See* art. 3 ("no state aircraft of a contracting state shall fly over the territory of another state or land thereon without authorization by special agreement or otherwise, and in accordance with the terns thereof.")

[55] *See* art. 16 ("[A]ir forces shall respect the air space over the Demilitarized Zone and over the area of Korea under the military control of the opposing side, and over the waters contiguous to both.")

[56] Stephen Townley, *Intervention's Idiosyncrasies: The Need for a New Approach to Understanding Sub-Forcible Intervention*, 42 Fordham Int'l L.J. 1167, 1174–1175 (2019).

[57] It seems to be a common misconception that the U.N. Charter expressly prohibits intervention. It does not. The word "intervention" only appears once in the Charter. *See* art. 2(7) ("[N] othing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state.") This passage prohibits the U.N. from intervening in private state matters but does not address interventions between individual states.

[58] G.A. Res. 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (Oct. 24, 1970).

[59] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. (June 27) ("*Nicaragua Case*"). It is worth noting that the *Nicaragua Case*, while routinely referenced by academics, is not necessarily binding on the United States. The United States has long rejected ICJ authority. The U.S. withdrew from the ICJ's compulsory jurisdiction in 1986, in response to the Nicaragua decision, and the Trump administration moved to withdraw from secondary treaties which may provide the court with indirect means of jurisdiction. Even so, U.S. officials have often cited to the *Nicaragua Case* as authoritative. *See, e.g.*, Egan, *supra* note 48.

[60] *Id.* at 97–98.

[61] Maneul Rodriguez, Disinformation Operations Aimed at (Democratic) Elections in the Context of Public International Law: The Conduct of the Internet Research Agency During the 2016 US Presidential Election, 47 Int'l J. Legal Info. 149, 167 (2019).

[62] Townley, *supra* note 56, at 1180.

[63] *Id*.

[64] It is debatable whether these prohibitions on interference also apply to questionable elections (e.g., Russia), one-party systems (e.g., China), or even monarchy-like hereditary systems (e.g., North Korea). This is particularly true of states which have not ratified the relevant human rights conventions. An assessment of these issues is beyond the scope of this article. To approach this potentially murky topic with caution, my argument in this article assumes that any stable government is protected from outside interference, and that it is the unlawful actions of such governments (genocide, aggression) which may be lawfully targeted by influence campaigns.

[65] Akande et al., *The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means*, Just Sec. (October 28, 2020), https://www.justsecurity.org/73097/oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means/ [https://perma.cc/8HGE-3LHQ].

[66] *Id.*

[67] *Id.*

[68] Rodriguez*, supra* note 61, at 168.

[69] *Nicaragua Case, supra* note 59, at ¶ 241.

[70] *Id.* ¶ 242.

[71] G.A. Res. 2625 (XXV), at 123 (Oct. 24, 1970).

[72] The court argued "the effect of consent to the text of such resolutions cannot be understood as merely that of a 'reiteration or elucidation' of the treaty commitment undertaken in the Charter. On the contrary, it may be understood as an acceptance of the validity of the rule or set of rules declared by the resolution by themselves." *Nicaragua Case*, *supra* note 59, at ¶ 188.

[73] Townley, *supra* note 56, at 1190.

[74] *Nicaragua Case*, supra note 59, at ¶ 205.

[75] *Id. See also* Townley, *supra* note 56, at 1171 (suggesting that the court may have meant "to leave open the possibility of taking a case-by-case approach" in assessing which actions constitute coercion).

[76] *See* Townley, *supra* note 56, at 1178-79. Townley also notes that "a number of Latin American states were among those that pushed the view that economic coercion should be considered aggression." *Id.* at 1185.

[77] Rodriguez, *supra* note 61, at 169.

[78] *Id.* at 168.

[79] Hollis, *supra* note 19, at 41.

[80] *See id.*

[81] *Id.* at 40–41. *See also* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired (21 Aug. 2007), https://www.wired.com/2007/08/ff-estonia/ [https://perma.cc/EV5N-GWLD] (providing background on the Estonia hack).

[82] *Id.* at 36.

[83] *See, e.g.*, Christopher J. Watterson, *Maximum Pressure Made Permeable: The Trouble with Washington's North Korea Sanctions*, War on the Rocks (24 Jan. 2020), https://warontherocks.com/2020/01/maximum-pressure-made-permeable-the-trouble-with-washingtons-north-korea-sanctions/ [https://perma.cc/HL5Z-P7B3].

[84] *See, e.g.*, Shawn Creamer, *Theater–Level Command and Alliance Decision-making Architecture in Korea*, 20 Int'l *J. Korean Stud. 2 (Fall 2016).*

[85] Shawn Creamer, *The Case for a Different Approach to Confronting North Korea*, Small Wars J. (Jul. 1, 2020), https://smallwarsjournal.com/jrnl/art/case-different-approach-confronting-north-korea [https://perma.cc/7HP6-PMTK].

[86] *Id.*

[87] The phrase "lean forward operationally" is borrowed from a former Judge Advocate for whom I had the privilege of working, whose mantra was "lean forward operationally and lean back fiscally." He would, however, be the first to admit that there are certain hard lines for which there is simply no "path to yes."

[88] Ney, *supra* note 51.

[89] *See* Seimghyun Sally Nam, *War on the Korean Peninsula? Application of Jus in Bello in the Cheonan and Yeonpyeong Island Attacks*, 8 E. Asia L. Rev. 43 (2013). Nam's analysis of when and how armistice can result in the full cessation of war is exceptional, noting that "modern armistice agreements are held to terminate war under international law; consequently, absent special circumstances, jus in bello should not apply and belligerent rights should not be recognized, since the parties have signed an armistice agreement." *Id*. at 70. However, the author's ultimate conclusions about the state of war on the Korean Peninsula seem to spin in the opposite direction of the analysis and are not well developed or supported. Separately, the question of whether the Korean Peninsula is currently at war is beyond the scope of this article. Current scholarship does mostly tend to conclude that no active armed conflict exists in Korea today[ ]. For the purpose of this case study, I adopt a presumption that peacetime legal regimes are applicable to Korea.

[90] Creamer, *supra* note 85.

[91] *Friendly Relations Declaration*, *supra* note 58.

[92] David Albright et al., *Alleged Sanctions Violations of UNSC Resolutions on North Korea for 2019/2020: The number is increasing*, Inst. for Sci. & Int'l Sec. (Jul. 1, 2020), https://isis-online.org/isis-

reports/detail/alleged-north-korea-sanctions-violations-2020/ [https://perma.cc/33UH-VPHV].

[93] The White House, *supra* note 8, at 14.

[94] *Senior U.S. Official Accuses China of Aiding North Korea Cyber Thefts*, Reuters (Oct. 23, 2020), https://www.reuters.com/article/us-usa-northkorea-china-idUSKBN2772RX [https://perma.cc/4USU-6JCX].

[95] *See* Katherine Zimmerman & Nicholas A. Heras, *Yemen Has Become an Iranian Proxy War Against Israel*, Foreign Policy (January 24, 2022), https://foreignpolicy.com/2022/01/24/yemen-houthi-uae-israel-iran-abraham-accords [https://perma.cc/K93F-74K2].

[96] *See* Bonnie S. Glaser, *Time for Collective Pushback Against China's Economic Coercion*, Ctr. for Strategic & Int'l Stud. (Jan., 2021), https://www.csis.org/analysis/time-collective-pushback-against-chinas-economic-coercion.

[97] Michael Birnbaum & Craig Timberg, *E.U.: Russians Interfered in Our Elections Too*, Wash. Post, June 14, 2019, https://www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too [https://perma.cc/UG52-W8G3].

[98] Neil Thurgood, *Hypersonics by 2023*, Army.Mil (Sep. 4, 2019), https://www.army.mil/article/226678/hypersonics_by_2023 [https://perma.cc/X2A9-4TY9].

[99] Dep't of Def., *supra* note 10, at 3.

[100] *See, e.g.,* Jude Blanchette & Seth G. Jones, *The U.S. Is Losing the Information War with China*, Wall St. J. (Jun. 16, 2020), https://www.wsj.com/articles/the-u-s-is-losing-the-information-war-with-china-11592348246 [https://perma.cc/8GQ6-62QK]; David Ignatius, *Why America is losing the information war to Russia*, Wash. Post (Sep. 4, 2019), https://www.washingtonpost.com/opinions/why-america-is-losing-the-information-war-to-russia/2019/09/03/951f8294-ce8e-11e9-b29b-a528dc82154a_story.html [https://perma.cc/HXA5-M792].

[101] Statement of General Richard D. Clarke, U.S Army, Commander, United States Special Operations Command, Before the House Armed Services Committee (Apr. 9, 2019), https://armedservices.house.gov/_cache/files/7/9/7970f176-0def-4a2d-beb3-a7d5d69e513b/9C80F888EEE40D8E82ABFF5336C012C3.hhrg-116-as26-wstate-clarker-20190409.pdf [https://perma.cc/T3RA-MANE].

[102] Patrick Tucker, *Should the US Have a Secretary For Influence Operations?,* Def. One (Feb. 22, 2020), https://www.defenseone.com/technology/2020/02/should-us-have-secretary-influence-operations/163272/ [https://perma.cc/5WHS-39UX].

[103] *See, e.g.* Alicia Wanless and James Pamment, *How Do You Define a Problem Like Influence?*, 18 J. Info. Warfare, at 5 (Winter 2019) ("Many terms used to describe the shaping of the information environment, such as 'propaganda' and 'information warfare', have pre-existing connotations that render them confusing for use in policy. These concepts also tend to be extremely broad, making it difficult to discern lines between what makes one type of communication acceptable and another

not... Propaganda is a prime example of this. Propaganda, in the most neutral sense, means to disseminate or promote particular ideas with the aim of manipulating a target audience into a behavior as desired by the propagandist. Propaganda is an agnostic tactic. As such, propaganda is an exceptionally broad concept, difficult to distinguish (if at all) from advertising, marketing, and public relations." (internal citations omitted)).

[104] *See* Memorandum from James Mattis, Sec'y of Def., to All Department of Defense Employees (August 4, 2017), https://dod.defense.gov/Portals/1/Documents/pubs/Ethical-Standards-for-All-Hands-SecDef-04-Aug-17.pdf [https://perma.cc/8VGL-R4S3].

Author

Author Publications

Justin Malzac

Justin Malzac is the Senior Paralegal at a DOD joint command and has been working in the national security law field for almost ten years. He has an M.A. in History from Pittsburg State University, a B.A. in English from the University of Minnesota, and was previously published in the *National Security Law Brief* and the *International Journal of Korean Studies.*

The Harvard National Security Journal

The Harvard National Security Journal (NSJ) is the nation's leading journal in the field of national security and law. The main edition publishes scholarly, practical articles by professors, legal practitioners, and national security professionals twice a year. The online edition publishes scholarly essays throughout the academic year.